



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G07F 7/10		A1	(11) International Publication Number: WO 99/45507
			(43) International Publication Date: 10 September 1999 (10.09.99)

<p>(21) International Application Number: PCT/US99/04986</p> <p>(22) International Filing Date: 5 March 1999 (05.03.99)</p> <p>(30) Priority Data: 09/035,647 5 March 1998 (05.03.98) US</p> <p>(71) Applicant (for all designated States except US): VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US).</p> <p>(72) Inventor; and (75) Inventor/Applicant (for US only): SLOAN, Jerry, F. [US/US]; 19968 Charters Avenue, Saratoga, CA 95070 (US).</p> <p>(74) Agent: SCOTT, Jonathan, O.; Beyer & Weaver, LLP, 620 Hansen Way, Palo Alto, CA 94306 (US).</p>	<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>
---	---

(54) Title: A SYSTEM AND METHOD FOR LOCKING AND UNLOCKING AN APPLICATION IN A SMART CARD

(57) Abstract

Locking and unlocking an application in a smart card (1208) allows for automatic authenticity of a lock or unlock command without the need for a personal identification number (PIN). The smart card (1208) is locked and unlocked by using a smart card device (1200, 1200a, 1200b) that need not have a keypad. The smart card device is a dedicated reader and locking/unlocking device, or can be a bank terminal, PC, telephone, etc. The smart card (1208) is inserted into the smart card device (1200, 1200a, 1200b). A lock command is sent from the device to the smart card. An application on the smart card is locked. The smart card (1208) sends identifying information, such as a password (PWD) and a card identification number (CID), to the device (1200) which is stored in a cache (506). The identifying information allows automatic authentication for unlocking of the card at a later time. The locked application cannot be used until it is unlocked. To unlock, the smart card (1208) is inserted into the device (1200) and an unlock button (1204) is pressed. The smart card device reads the card identification number of the card and determines if the corresponding password for that card is present in the cache of the device. If so, an unlock command is issued to the smart card along with the password. If the password received by the smart card matches the password of the smart card then the smart card is unlocked.

```

graph TD
    1200[1200] --- 500[MICROPROCESSOR]
    500 <--> 502[DISPLAY]
    500 <--> 506[CACHE]
    500 <--> 504[ROM]
    500 <--> 510[FUNCTION BUTTON(S)]
    500 <--> 508[CARD READER]
  
```

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

A SYSTEM AND METHOD FOR LOCKING AND UNLOCKING AN APPLICATION IN A SMART CARD

5

FIELD OF THE INVENTION

The present invention relates generally to smart card transactions, more particularly, to a system and method for locking and unlocking an application in a smart card.

BACKGROUND OF THE INVENTION

A smart card is typically a credit card-sized plastic card that includes a semiconductor chip
10 capable of holding data supporting multiple applications. One popular such application is the holding of the digital equivalent of cash directly, instead of pointing to an account or providing credits. Accordingly, smart cards with such an application are also sometimes referred to as stored-value cards. When a card of this kind is used to make a purchase, the digital equivalent of cash is transferred to the merchant's "cash register" and then to a financial institution.
15 Stored-value cards are either replenishable (value can be reloaded onto the card using a terminal) or non-replenishable (the card is decremented in value for each transaction and thrown away when all its value is gone).

Physically, a smart card often resembles a traditional "credit" card having one or more semiconductor devices attached to a module embedded in the card, providing contacts to the
20 outside world. The card can interface with a point-of-sale terminal, an ATM, or a card reader integrated into a telephone, a computer, a vending machine, or any other appliance. A micro-controller semiconductor device embedded in a "processor" smart card allows the card to undertake a range of computational operations, protected storage, encryption and decision making. Such a micro-controller typically includes a microprocessor, memory, and other
25 functional hardware elements. Various types of cards are described in "The Advanced Card Report: Smart Card Primer", Kenneth R. Ayer and Joseph F. Schuler, The Schuler Consultancy, 1993.

One example of a smart card implemented as a processor card is illustrated in FIG. 1. Of course, a smart card may be implemented in many ways, and need not necessarily include a microprocessor or other features. The smart card may be programmed with various types of functionality, including applications such as stored-value; credit/debit; loyalty programs, etc.

5 For the purpose of this disclosure, card 5 is programmed with at least one application such as stored value application, and may be referred to as "stored-value" card 5.

Stored-value card 5 has an embedded micro-controller 10 that includes a microprocessor 12, random access memory (RAM) 14, read-only memory (ROM) 16, non-volatile memory 18, an encryption module 22, and a card reader interface 24. Other features of the micro-controller
10 may be present but are not shown, such as a clock, a random number generator, interrupt control, control logic, a charge pump, power connections, and interface contacts that allow the card to communicate with the outside world.

Microprocessor 12 is any suitable central processing unit for executing commands and controlling the device. RAM 14 serves as storage for calculated results and as stack memory.
15 ROM 16 stores the operating system, fixed data, standard routines, and look up tables. Non-volatile memory 18 (such as EPROM or EEPROM) serves to store information that must not be lost when the card is disconnected from a power source but that must also be alterable to accommodate data specific to individual cards or any changes possible over the card lifetime. This information might include a card identification number, a personal identification number,
20 authorization levels, cash balances, credit limits, etc. Encryption module 22 is an optional hardware module used for performing a variety of encryption algorithms. Card reader interface 24 includes the software and hardware necessary for communication with the outside world. A wide variety of interfaces are possible. By way of example, interface 24 may provide a contact interface, a close-coupled interface, a remote-coupled interface, or a variety of other interfaces.
25 With a contact interface, signals from the micro-controller are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device.

A smart card can include multiple applications, including, for example, applications such as credit, debit, stored value, telephone, or loyalty. Given such a multi-application smart card, a
30 problem could arise when the smart card is given to a service provider for a single transaction.

For example, the owner of the smart card may give the smart card to a waiter in a restaurant for a credit transaction. However, without a means for locking the other applications, such as the stored value or telephone applications, the waiter has access to all of the applications, such that the waiter could possibly make phone calls or conduct stored value transactions with the smart card during the time it is in his possession.

A solution to this problem includes the use of a device, commonly referred to as an "electronic wallet", into which a smart card can be inserted and a particular application can be locked such that a particular application cannot be used until it is unlocked. Some smart card companies, such as Mondex International, currently utilize a wallet which can lock and unlock a smart card. The locking and unlocking mechanism utilizes a personal identification number (PIN) to ensure authenticity of the lock or unlock request. However, many people prefer not to use PINs. It is a nuisance to have to memorize a PIN, particularly if the person already has several PINs memorized. Additionally, a particular PIN can be forgotten or confused with another PIN. Further, the need for a PIN requires that the "electronic wallet" device has at least a numeric key pad to enter the PIN. This is undesirable for some users who do not want to carry a relatively bulky wallet with them.

What is needed is a system and method for automatically ensuring authenticity for locking and unlocking an application in a smart card which does not require the user to memorize a PIN. Preferably, the system and method may be implemented using a device which does not require the use of a bulky and expensive keypad. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The present invention provides a system and method for locking and unlocking an application in a smart card. The system and method according to the present invention allows for automatic determination of the authenticity of a lock or unlock command without the need for a personal identification number. The smart card can be locked and unlocked by utilizing a smart card device. The smart card can be inserted into the smart card device to lock at least one application of the smart card such that the locked application cannot be utilized until it is unlocked. During the locking process, the smart card sends identifying information, such as a password and card ID, to the smart card device to allow automatic authentication for unlocking

of the card at a later time. A password is herein meant to include a combination of characters which can include letters, numbers, and various symbols.

To unlock an application in a smart card, the smart card device identifies the card and looks for the password corresponding to this particular card. If the password is found in the smart card device's cache memory, then the password and an "unlock" command are issued from the smart card device to the smart card. When the smart card device receives the password along with the unlock command, it is determined whether the received password matches the actual password for the smart card. If the passwords match, then the application is unlocked.

A system and method according to the present invention for locking and unlocking an application in a smart card uses a smart card device. The method for unlocking the application comprises the steps of automatically determining a first password; determining whether the first password matches a second password; and unlocking the application if the first password matches the second password. Further, the method according to the present invention for locking the application comprises the steps of sending a command to lock the application in the smart card; sending smart card identifying information to a smart card device; and locking the application in the smart card.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

FIG. 1 is a block diagram of an example of a conventional smart card.

FIG. 2 is a block diagram of a conventional wallet.

FIG. 3 is a flow diagram of a conventional method for locking an application in a smart card.

FIG. 4 is a flow diagram of a conventional method for unlocking an application in a smart card.

FIGS. 5A and 5B show examples of a smart card device according to embodiments of the present invention.

FIG. 6 is a block diagram of a smart card device according to an embodiment of the present invention.

5 FIG. 7 is an example of a cache which may be used in conjunction with the smart card device shown in FIG 6.

FIG. 8 is a flow diagram of a method according to an embodiment of the present invention for locking an application in a smart card.

10 FIG. 9 is a flow diagram of a step of storing information in a cache as described in the method shown in FIG 8.

FIGS. 10A-10C depict the International Standards Organization format for the command, response, and command header for information conveyed to and from the smart card.

FIGS. 11A-11C are tables illustrating examples of the command, response, and return codes for the lock application command.

15 FIG. 12 is a flow diagram of a method according to an embodiment of the present invention for unlocking an application in a smart card.

FIGS. 13A-13B show tables describing the command and return codes for the unlock command.

20

DETAILED DESCRIPTION OF THE INVENTION

While this invention is described in terms of several preferred embodiments, it is contemplated that alternatives, modifications, permutations and equivalents thereof will become apparent to those skilled in the art upon a reading of the specification and study of the drawings.

FIG. 2 shows a block diagram of a conventional electronic wallet 210. This example of a conventional wallet includes a display 200, a microprocessor 202, a read only memory (ROM) 204, a card reader 206, and a numeric pad with special function buttons 208. Typically, a user can insert a smart card into a wallet such as that shown in FIG. 2 and information, such as the amount of value remaining in a stored value application of the card, can be displayed on the display 200. The numeric pad and special function buttons 208 can be used by the user to input a PIN in order to access the information. Numeric pad and special function buttons 208 may also include a "lock" button (not shown) for locking a card. A separate "unlock" button may also be included or it may be the same button as the "lock" button.

FIG. 3 shows a flow diagram of a conventional method for locking an application in a smart card. The smart card is inserted into a device such as an electronic wallet, an automated teller machine (ATM), or an input device to a computer system. In this example, a conventional electronic wallet 210 will be used. A lock button is pressed by the user (step 302) and wallet 210 sends a lock command to the smart card (step 304). The smart card, in response to the lock command, then locks an application in the smart card (step 306).

FIG. 4 shows a flow diagram of a conventional method for unlocking an application in a smart card. The smart card is inserted into an electronic wallet (e.g., wallet 210) (step 400), and an unlock button is then pressed (step 402). The wallet typically prompts the user to enter a PIN (step 404). The user then enters the PIN (step 406). The wallet sends an unlock command to the smart card wherein the PIN is included in the unlock command (step 408). The smart card then unlocks an application in step 410 if the PIN sent by the wallet is correct.

One of the problems with these conventional methods of locking and unlocking an application for a smart card as described in FIGS. 3 and 4, is that the user is required to memorize a personal identification number (PIN). Many people find having to memorize a PIN a nuisance. This nuisance can be further compounded by the need to keep track of a number of different PINs for, e.g., a bank account, a password at work, etc. The user may choose to have a different PIN for every different type of transaction which requires a PIN, or select a single PIN to apply to all transactions in his life. However, if the user is required to memorize numerous PINs for numerous activities, then the user also needs to remember which PIN applies to which transaction. If the user selects a single PIN for all of his transactions, then the user has a higher

risk of exposing his PIN. This problem may become even greater if different applications on a single smart card require different PINs.

Accordingly, what is needed is a system and method for locking and unlocking an application in a smart card which does not require the user to memorize a PIN. Embodiments of the present invention address such a need.

The method and system according to embodiments of the present invention provides a lock/unlock feature of an application in a smart card wherein the transaction is automatically authenticated. Additionally, embodiments of the present invention provide the ability to lock/unlock an application, such as a stored value application (sometimes referred to as a "purse"), using one of a plurality of smart card devices which can lock/unlock a particular smart card. An application in a particular smart card may also be locked with a first one of a plurality of smart card devices and unlocked with a second one of the plurality of smart card devices. In one embodiment of the present invention, the issuer of the smart card can also unlock an application in a smart card if a smart card device is unable to do so. For example, in one embodiment, the smart card issuer can look up or regenerate the unique password assigned to the particular smart card and have it downloaded to a terminal device, such as the cardholder's personal computer system.

FIGS. 5A and 5B show examples of two embodiments of smart card devices 1200a and 1200b according to the present invention. Smart card device 1200a is shown to be approximately a little larger than the smart card 1208. Smart card device 1200a includes a display 1202a, at least one function button 1204, and a card slot 1206a. Display 1202a can be used to display card value amounts such as monetary value or credit value, or other information such as the last ten transactions performed by the smart card, or the like. Special function button 1204 can be a button dedicated for use in issuing a lock command or an unlock command. Alternatively, special function button 1204 can represent more than one function, for instance button 1204 can be pressed twice for unlock and once for lock. Smart card device 1200a also includes a slot 1206a into which smart card 1208 is inserted. Another possible example is to have smart card device 1200b attached to a key chain 1220. This type of smart card device would still include a display 1202b and an insert slot 1206b. Smart card 1208' can simply be partially inserted into smart card device 1200b and the pressure of the insertion of smart card

1208' against internal contacts (not shown) can initiate functions such as a lock or unlock command.

FIG. 6 is a block diagram of a smart card device according to an embodiment of the present invention. It shows a microprocessor 502 coupled with a display 500, a memory such as a ROM 504, function button(s) 510, a card reader 508, and a cache 506. Microprocessor 502 can accept input from both function button(s) 510 and card reader 508. It can then access information from ROM 504 and access data from cache 506. Various messages, such as "locked", "unlocked", available balance, and the last few transactions can be displayed on display 500.

FIG. 7 shows an example of cache 506. Cache 506 can be a non-volatile memory such as an EEPROM or a FLASH memory. Preferably, cache 506 can include several passwords associated with several smart cards. Although the cache can contain a single password associated with a single smart card, the retention of several passwords associated with several smart cards allows for the flexibility of utilizing the same smart card device with several different smart cards. Those skilled in the art will recognize that cache 506 may be used to store other information as well. A card identification number (CID) assigned to each smart card uniquely identifies each smart card. Cache 506 can include a list of smart cards used in the most recent transactions. For example, the last ten smart cards utilized with a particular smart card device can be listed under CID, preferably with the most recent transaction listed at the top with the oldest transaction listed at the bottom. Associated with the CID are the passwords (PWD) listed in the same order. Accordingly, the first card ID and its associated password would be listed at the top of the list while the card ID of the smart card which was used in the oldest transaction and its password would be listed at the bottom of the list. When the cache is full, then the card ID and its associated password which is listed at the bottom of the list, i.e., the card which was used in the oldest transaction, would be removed. Further details regarding the generation and use of the CID and PWD will be given below.

According to embodiments of the present invention, during personalization or initialization of smart card 1208, the card issuer generates a derived password based on the card number and a master key. This password could be given to the cardholder, but the cardholder will most likely not need to memorize it for normal operation. The password is stored in smart

card 1208 and is preferably not retrievable externally without using smart card device 1200 which can lock or unlock an application in smart card 1208. Upon reading this disclosure, those skilled in the art will recognize that entities other than the "card issuer" may be responsible for generating the derived password for use in the present invention. For example, an agent of the card issuer may generate the password. For simplicity, however, this specification will continue to refer to the "card issuer" as the entity generating a password.

There are many ways to generate a password for smart card 1208. One example of a method which can be used by the card issuer for generating a password for a card includes the use of Data Encryption Standard (DES) algorithm. The issuer can generate a DES cryptogram using a DES algorithm and a secret key. The issuer can encipher a unique serial number or identification number of the card and provide a unique binary number for each card. The binary number can be converted to a decimal number and a predetermined number of digits, such as the last six digits, can be used to produce a unique password for the smart card 1208.

To lock an application, the cardholder can place smart card 1208 into smart card device 1200 and request a locking function, for example, by pressing special function lock button 1204. Once the application is locked, the card can be safely given to another person, such as a waiter in a restaurant. When the card is returned, the cardholder can put smart card 1208 back into smart card device 1200 and press the unlock button, e.g., item 1204, to unlock the application which was previously locked. The smart card device reads the card ID from the card and uses the card ID to find the matching card ID and associated password in the cache 506 of smart card device. Smart card device 1200 then sends the password to smart card 1208 in an unlock command to unlock the locked application.

If the card holder forgets to bring his own smart card device 1200, he can borrow one from a family member or another trusted party. Any smart card device implemented with features of the present invention can lock any application in any smart card which has also been implemented in accordance with the present invention. Additionally, any smart card device 1200 according to the present invention that has previously locked a specific application in a specific smart card 1208 can unlock that application (within the limit of the cache storage capacity of the smart card device). If a card holder borrows a smart card device 1200 from a friend to lock an application in his smart card, the application can be unlocked with the friend's

smart card device or with the cardholder's smart card device. This system and method allows family members or close friends to share smart card devices 1200 if they wish.

Any smart card device 1200 implemented according to the present invention which has the appropriate password for unlocking a given smart card application can unlock the application by sending an unlock command to the card. Normally, this will be done by the same smart card device that was used to lock the application in the smart card. If that smart card device is not available, the application in the smart card can be unlocked via a bank terminal, a PC, a telephone, or virtually any device with the capability to read and write information to a smart card, so long as the device is provided with the functionality described herein (e.g., the ability to generate lock and unlock commands per the present invention).

If required, (after appropriate identification), the password can be obtained from the card issuer after being easily generated by numerous well-known methods, such as Data Encryption Standard (DES), given the card ID. For example, an ATM can be programmed to display "card unlocking" as an option to its list of services. A user can then select the "card unlocking" service and allow the ATM to read information, including card ID, from the card. If the ATM already has the required DES key stored in its memory, then the card's password can be generated by the ATM. More likely, however, the ATM will need to contact a host computer which has access to the appropriate DES secret key (e.g., based on the card number and issuer). The ATM can send the card ID to the host computer which can regenerate the card's password. Alternatively, the host computer can read the card's password from a database. The resulting password can be returned to the ATM which can send an unlock command to the card using the password. A similar unlocking transaction can occur using a bank terminal, a PC, a telephone, or virtually any device with the capability to read and write information to a smart card.

FIG. 8 shows a flow diagram of a method according to an embodiment of the present invention for locking an application in a smart card. Smart card 1208 is inserted into smart card device 1200 (step 700), and a card application is selected (step 701). Once a card application is selected, commands are directed toward the selected application thereafter. A lock request is indicated (step 702). A lock button or split function button 1204 can be pressed by the cardholder to indicate the lock request. Smart card device 1200 sends a lock command to the smart card (step 704). It is then determined if the application in smart card 1208 is already

locked (step 706). If it is locked then smart card device 1200 displays a message such as "locked" (step 708). Preferably, smart card device 1200 does not relock an application that has already been locked. Avoiding relocking an application that has already been locked ensures that no unauthorized person can simply relock the application thereby storing the password into his smart card device, then unlocking the application using the password which has just been stored.

If the application is not already locked (step 706) then the application is locked (step 710). Smart card 1208 sends the card identification (CID) and password (PWD) to smart card device 1200 (step 712). Smart card device 1200 then displays a predetermined message such as "OK" (step 714) and then smart card device 1200 stores the CID and associated PWD in its cache 506 (step 716).

FIG. 9 is a flow diagram for a method for storing information in cache 506 of smart card device 1200 as recited in step 716 of FIG. 8. The CID of the particular smart card is searched for in cache 506 of smart card device 1200 (step 800). If smart card device 1200 finds that the particular CID is in the cache (step 802), then that particular CID can be brought to the top of the list of CIDs (step 804). The list refers to the CID list shown in FIG. 7.

If the CID is not found in cache 506 (step 802), then it is entered in cache 506, preferably at the top of the CID list (step 806). It is determined if the cache is full (step 808) and if it is not then the process is complete (step 810). If, however, the cache is full then the bottom item on the list is removed (step 812). In this manner, a relatively small cache size can be used to store the most recently used CID information. Those skilled in the art will recognize that other list approaches may also be used.

FIGS. 10A-10C show the preferred format for the command response and command header used in locking and unlocking a smart card according to the present invention. The preferred format is described in detail by the International Standards Organization (ISO) which defines the specific format for the command. ISO standard 7816-4, "Information Technology - Identification Cards - Integrated Circuit Cards with Contact Part 4" is herein incorporated by reference.

FIG. 10A shows a currently preferred format for the command used to lock or unlock a card. The format includes a command header (HDR) 800, followed by a data field, followed by a trailer (Le). FIG. 10B shows a currently-preferred format for a response to the command which includes optional data followed by the status (SW1, SW2). FIG. 10C shows a currently preferred format of command header 800. The format for command header 800 includes a class byte (CLA) followed by the instruction code (INS). P1 and P2 are in the third and fourth byte positions with P1 and P2 varying depending on the specific instructions given. After P1 and P2, is a field indicating the length of command data (Lc).

FIGS. 11A-11C illustrate examples of the command, the response, and the return codes for performing a locking function according to an embodiment of the present invention. In this example, the preferred format from the above-described ISO standard is used. FIG. 11A shows an example of a lock command which will be issued by, e.g., a smart card device as shown in FIG. 5A or 5B. In this example of a lock command, the class field (CLA) has a content value of a hex number "80", which in this case indicates that it is not a standard ISO instruction. The instruction is identified as a lock command by a hex number, such as "FF", and P1 and P2 both have "00" which can indicate that no parameters are to be sent. For the response to a lock command shown in FIG. 11B, smart card 1208 will generate a message including the CID (5 bytes) and the password (3 bytes). The return codes shown in FIG. 11C which will be generated by the card will include status word one (SW1) and status word two (SW2) with values of "9000" or "9110". "9000" indicates a successful lock of the application, while "9110" indicates that the application is already locked.

FIG. 12 shows a flow diagram of a method according to the present invention for unlocking an application in a smart card 1208. Smart card 1208 is inserted into a smart card device 1200 in step 1000, and a card application is selected (step 1001). Once a card application is selected, commands are then directed to the selected application. An unlock button (or other means for initiating an unlock command) is then pressed (step 1002). The smart card device reads the CID in step 1004. Smart card device 1200 then determines whether the password associated with the CID is stored in the cache of the smart card device (step 1006). If the password is not stored in the cache then the smart card device is unable to unlock the smart card application and a message such as "unable to unlock" can be displayed (step 1008).

If, however, the password is found in the cache of smart card device 1200, then an "unlock" command is issued (step 1010). Smart card device 1200 then determines if the smart card application is already unlocked (step 1012). If the card application is already unlocked, then an error has occurred and an error message can be displayed to the card holder (step 1014).

- 5 If, however, the smart card application has not already been unlocked, then device 1200 determines whether the password sent to the smart card through the "unlock" command matches the password associated with the smart card (step 1016). If it does not, then an error has occurred and the smart card application is not unlocked (step 1018). If, however, the password sent from the smart card device to the smart card matches the password associated
10 with the smart card, then the application is unlocked (step 1020).

FIGS. 13A-13B illustrate an example of command and return codes for the unlock function. Again, it is preferable that the command formats set forth by the ISO standards be utilized. Accordingly, the example shown in FIG. 13A for the unlock command includes information related to the class, instruction, the parameters, and the length of data command.

- 15 The example of the return codes shown in FIG. 13B include status word one (SW1) and status word two (SW2) including "9000" implying successful operation, "9111" implying that the application has already been unlocked, and "9112" implying that the application could not be unlocked because the smart card device either did not have the password or the password was incorrect.

- 20 A method and system for locking and unlocking an application in a smart card has been disclosed. Software written according to the present invention may be stored in some form of computer-readable medium, such as in computer memory, on a floppy or hard disk, or on a CD-ROM, transmitted over a network, and/or executed by a processor.

- 25 Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

CLAIMS

1. A smart card device for unlocking an application in a smart card able to be inserted in said smart card device, said smart card device comprising:

a card reader arranged to read from and to write to said inserted smart card;

5 a memory coupled to said card reader, said memory including

a card identification number corresponding to said smart card, and

a password corresponding card identification number; and

a microprocessor coupled to said card reader, said microprocessor arranged to issue an unlock command along with said password to said smart card when said smart card provides
10 identifying information matching said card identification number, whereby said smart card device is able to unlock said application in said smart card.

2. A smart card device as recited in claim 1 further comprising:

a function button arranged to issue an unlock request to said microprocessor when activated.

15 3. A smart card device as recited in claim 1 further comprising:

a display for indicating a status of said smart card.

4. A smart card device as recited in claim 1 wherein said memory is a cache arranged to hold a plurality of card identification numbers and a corresponding plurality of passwords, whereby said smart card device may be used to unlock a plurality of applications.

20 5. A smart card device as recited in claim 4 wherein said microprocessor is further arranged to delete an oldest pair of corresponding card identification number and password when said cache is full.

6. A method of locking an application of a smart card using a smart card device, said method comprising:

receiving said smart card in said smart card device;

sending a lock command to said smart card intended for said application;

receiving identifying information from said smart card; and

storing said received identifying information in a memory of said smart card device,

5 whereby said application of said smart card may not be used until said application is unlocked.

7. A method as recited in claim 6 wherein said identifying information includes a password and a card identification number, whereby said card identification number may be used to find said password in said memory of said smart card device.

8. A method as recited in claim 6 further comprising:

10 receiving an unlock request; and

sending said identifying information from said memory to said smart card along with an unlock command, whereby said application of said smart card is unlocked and available for use.

9. A method as recited in claim 6 wherein said memory is implemented as a stack and wherein said element of storing includes:

15 determining whether said memory is full; and

wherein when it is determined that said memory is full, deleting other identifying information related to an oldest transaction of said smart card device.

10. A method as recited in claim 6 further comprising:

determining whether said application of said smart card has already been locked; and

20 wherein when it is determined that said application is already locked, said identifying information is not stored in said memory of said smart card device, whereby unauthorized unlocking is inhibited.

11. A method of unlocking an application of a smart card using a smart card device, said method comprising:

receiving said smart card in said smart card device;

receiving identifying information from said smart card;

searching a memory of said smart card device for said identifying information; and

sending an unlock command to said smart card intended for said application, whereby

5 said application of said smart card is unlocked and available for use.

12. A method as recited in claim 11 wherein said identifying information includes a card identification number, said method further comprising:

identifying a smart card password in said memory of said smart card device that corresponds to said card identification number; and

10 sending said smart card password to said smart card, whereby said smart card password is used by said smart card to verify that said unlock command from said smart card device is authorized.

13. A method as recited in claim 11 wherein said memory is implemented as a cache and wherein said method further comprises:

15 matching said identifying information with a password in said cache; and

sending said password to said smart card along with said unlock command, whereby said password is used by said smart card to verify that said unlock command from said smart card device is authorized.

14. A method of unlocking an application of a smart card using a computing device, said
20 method comprising:

receiving said smart card in said computing device;

receiving identifying information from said smart card;

automatically generating a password corresponding to said identifying information of said smart card; and

sending an unlock command along with said generated password to said smart card, whereby said password is used by said smart card to verify that said unlock command from said computing device is authorized.

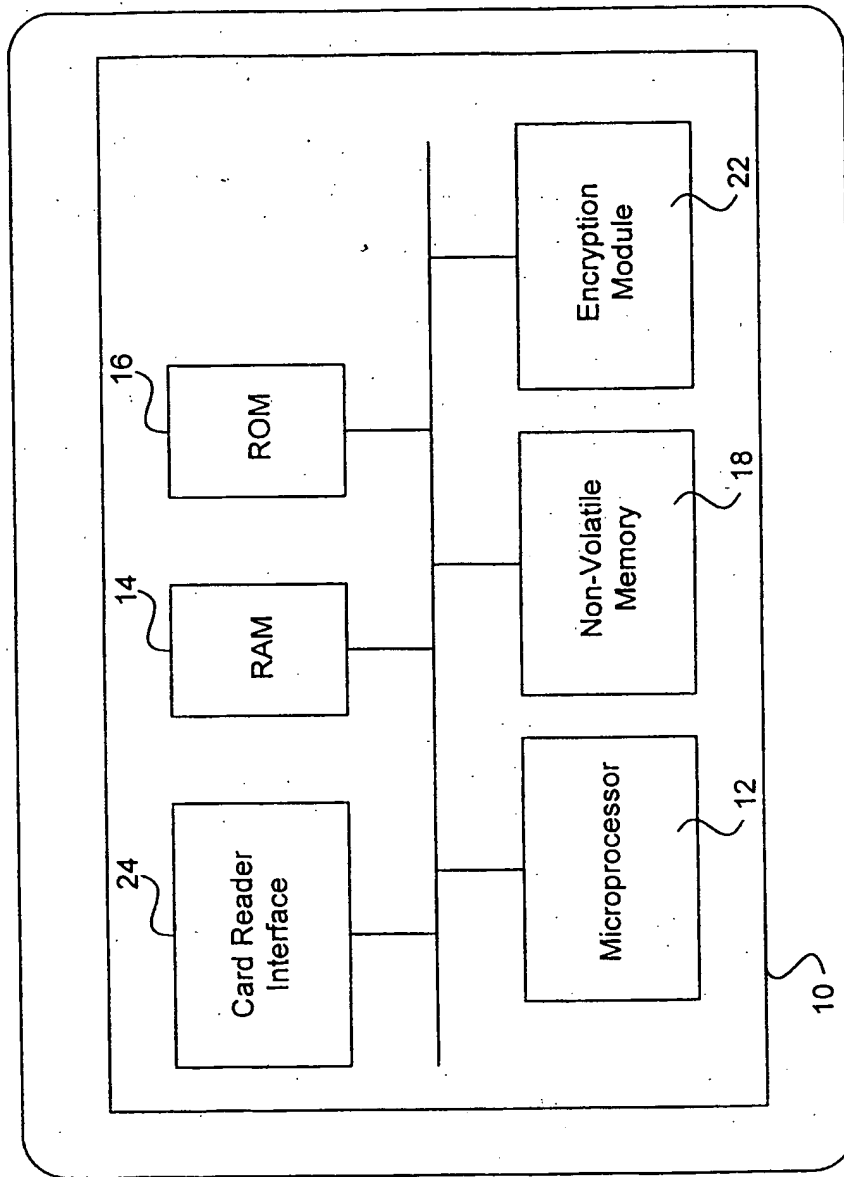
15. A method as recited in claim 14 wherein said computing device is a bank terminal, a personal computer, a telephone, or an automated teller machine.

16. A method as recited in claim 14 wherein said password is generated by referencing a memory of said computing device using said identifying information.

17. A method as recited in claim 14 wherein said identifying information includes a card identification number, and said element of automatically generating includes:

using a cryptographic technique to generate said password based upon said card identification number, whereby said password need not be stored by said computing device.

5



Stored-Value Card Example

FIG. 1
(PRIOR ART)

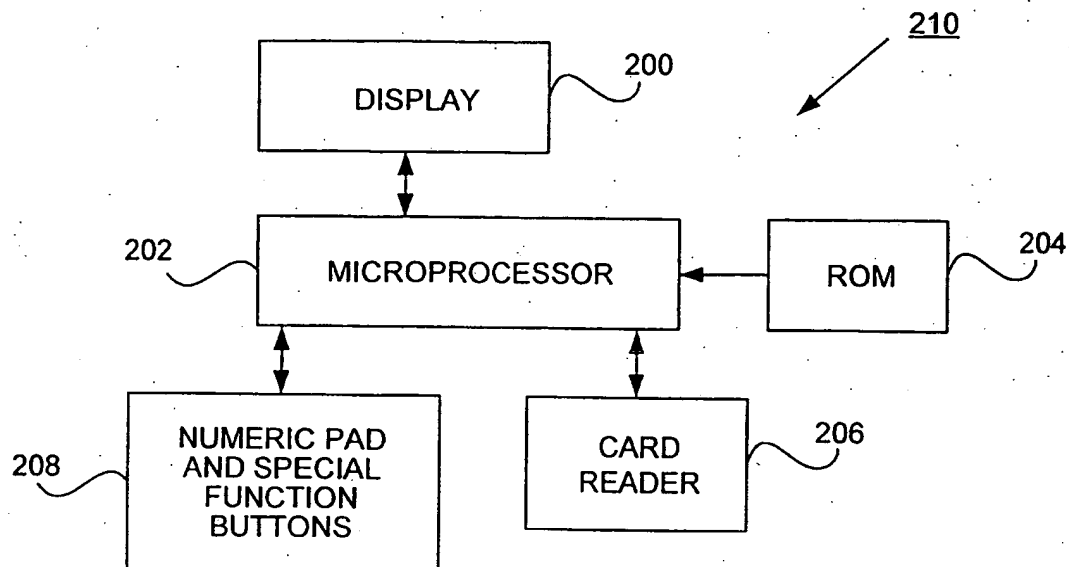


FIG. 2
(PRIOR ART)

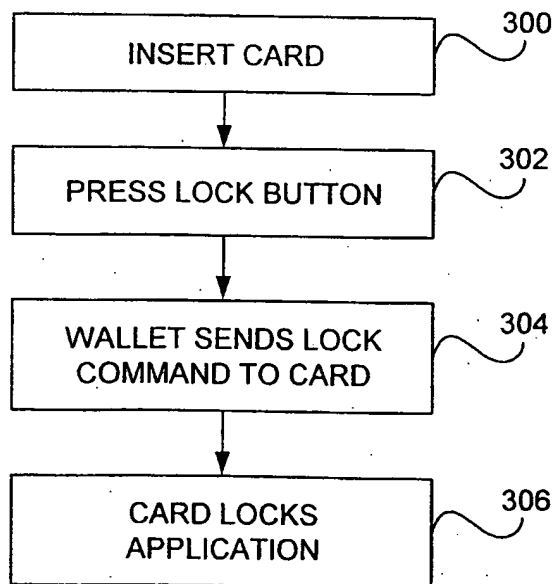


FIG. 3
(PRIOR ART)

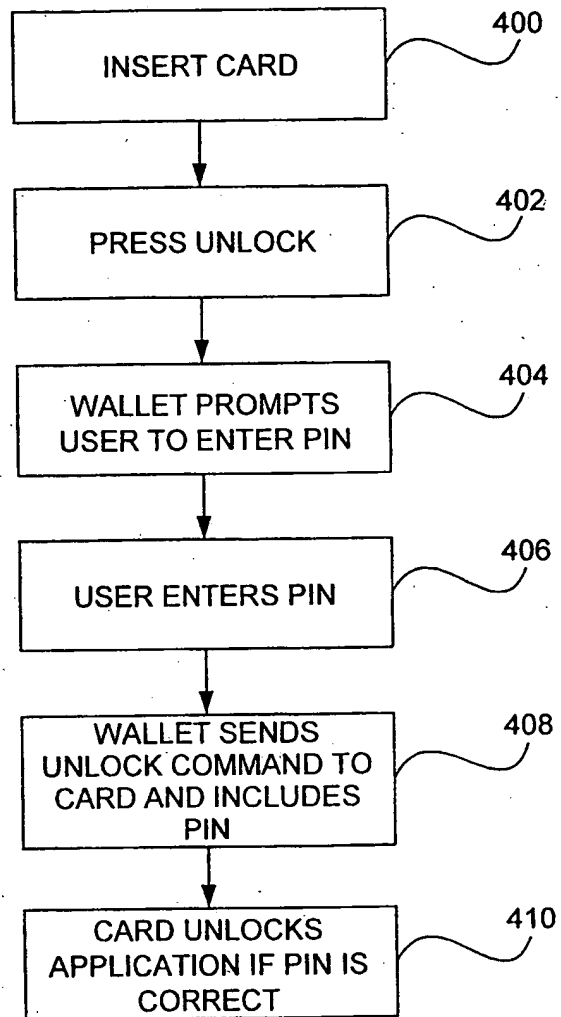
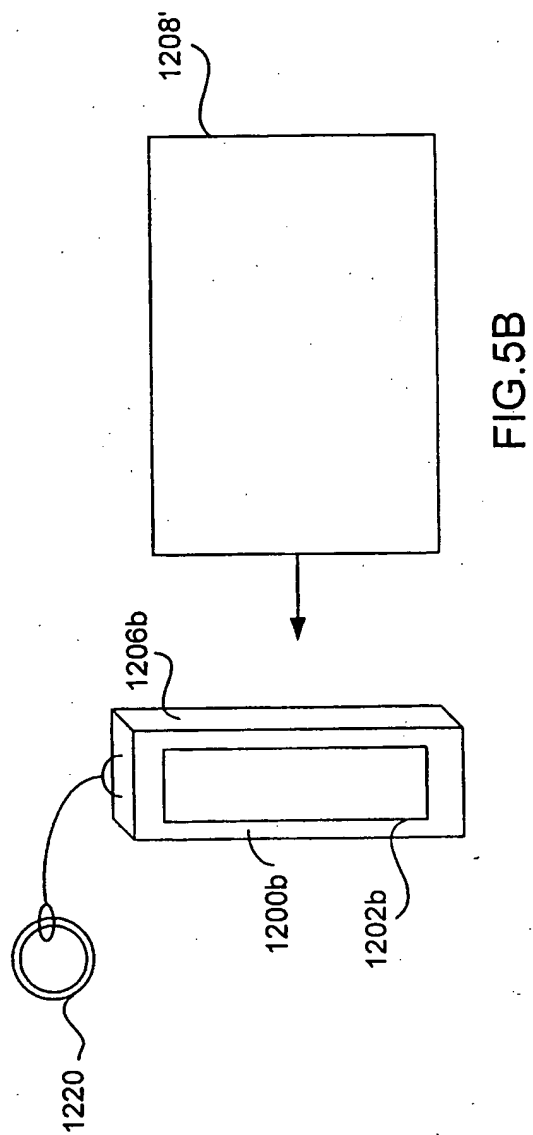
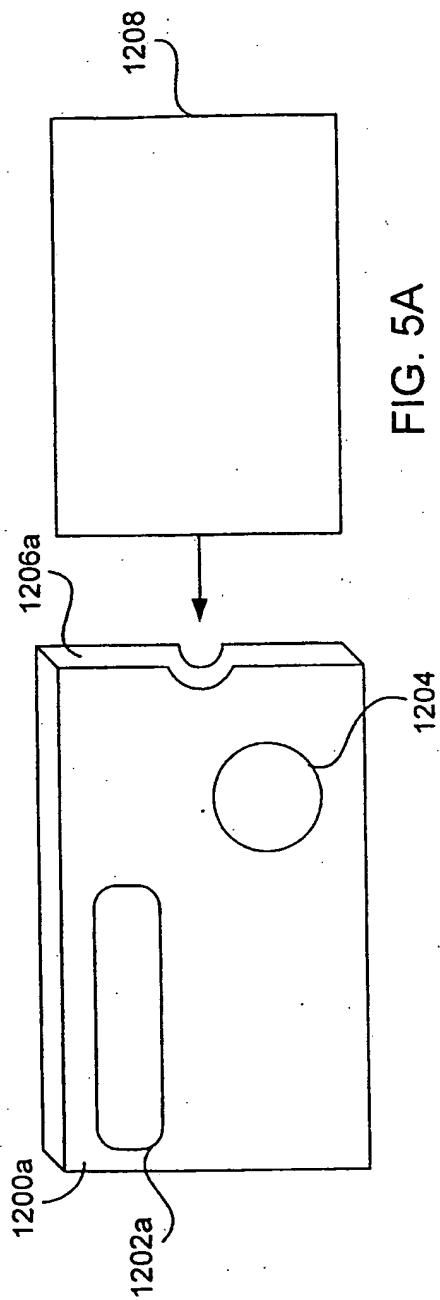


FIG. 4
(PRIOR ART)



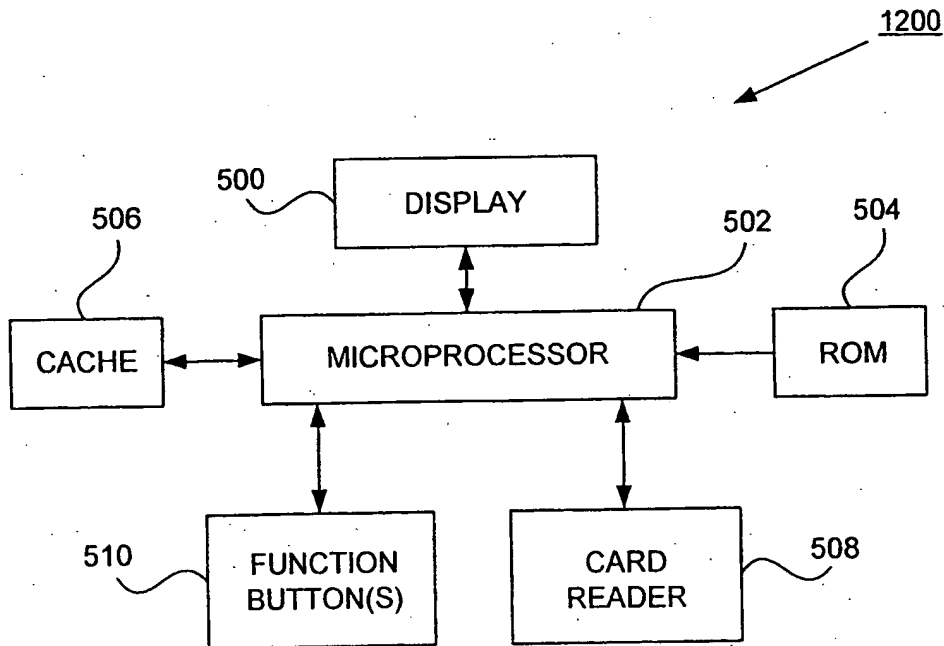


FIG. 6

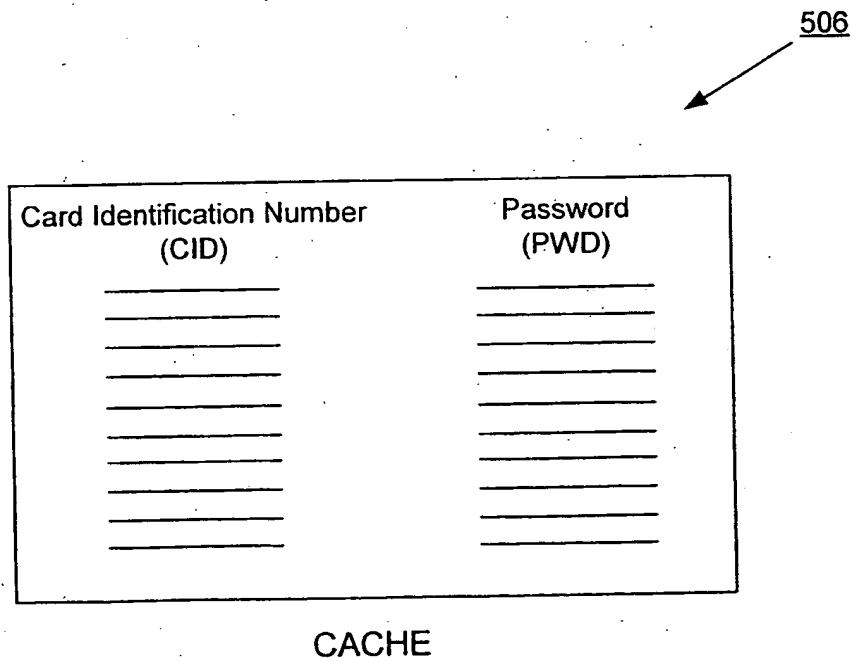


FIG. 7

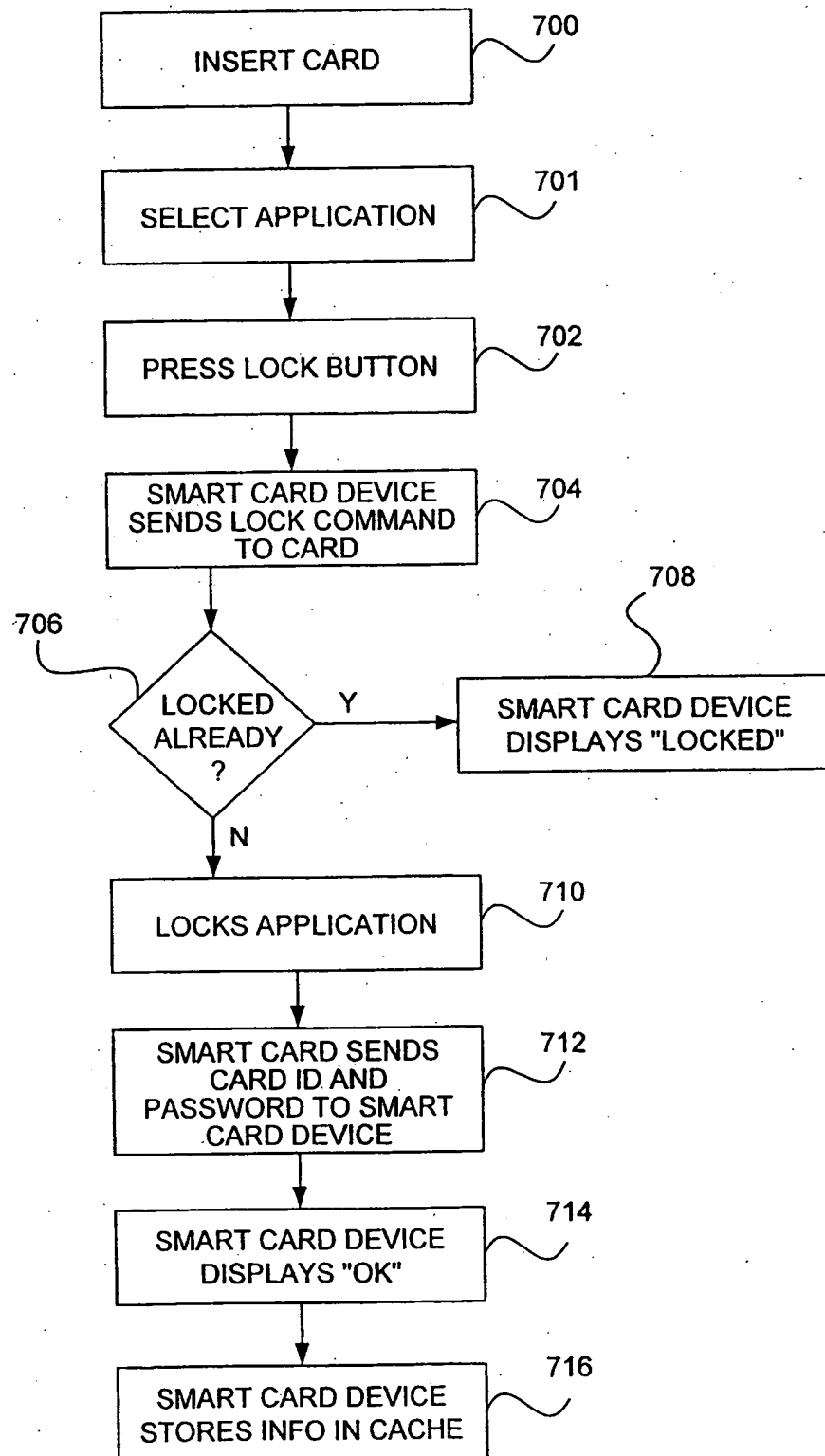


FIG. 8

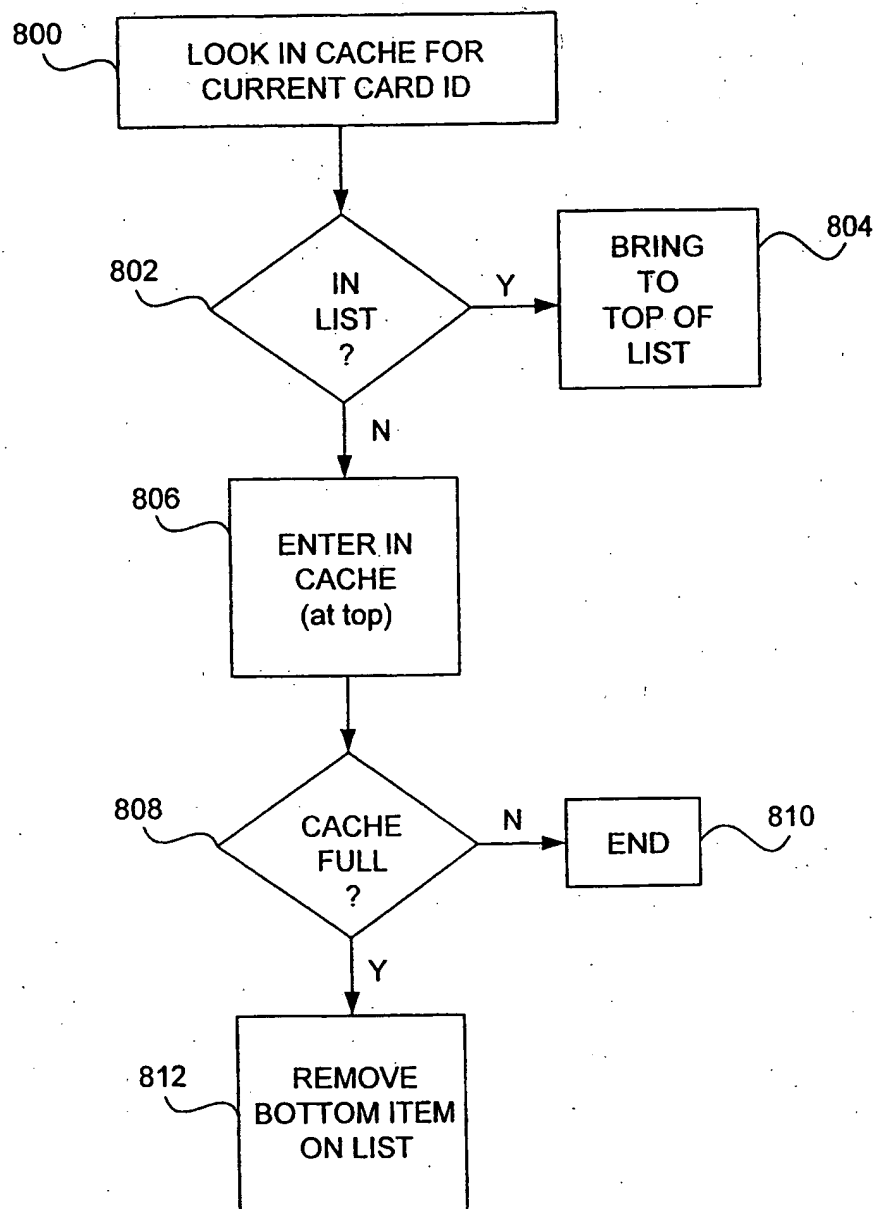
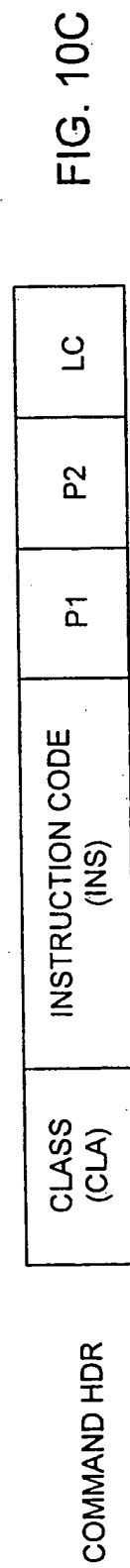
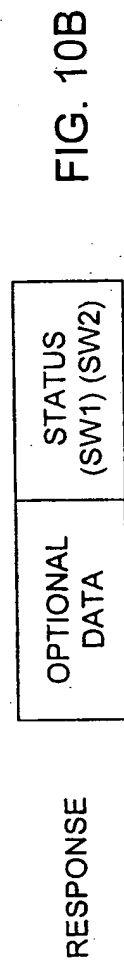
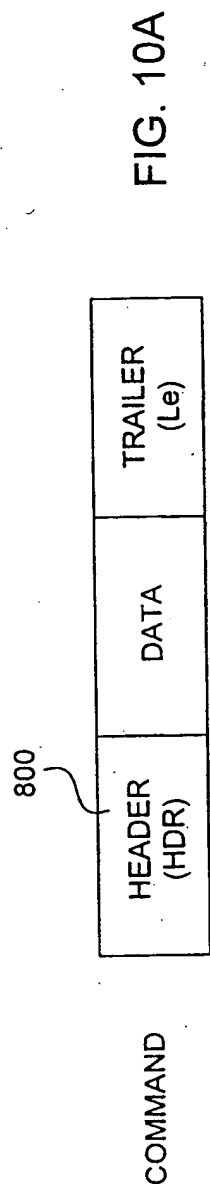


FIG. 9



COMMAND LOCK

	CONTENT	LENGTH
CLA	'80'	1
INS	TBD	1
P1	'00'	1
P2	'00'	1

FIG. 11A

RESPONSE LOCK

RESPONSE DATA	LENGTH
CARD ID	5
PASSWORD	3

FIG. 11B

RETURN CODES

SW1	SW2	MEANING
'9000'		SUCCESSFUL OPERATION
'9110'		APPLICATION LOCKED

FIG. 11C

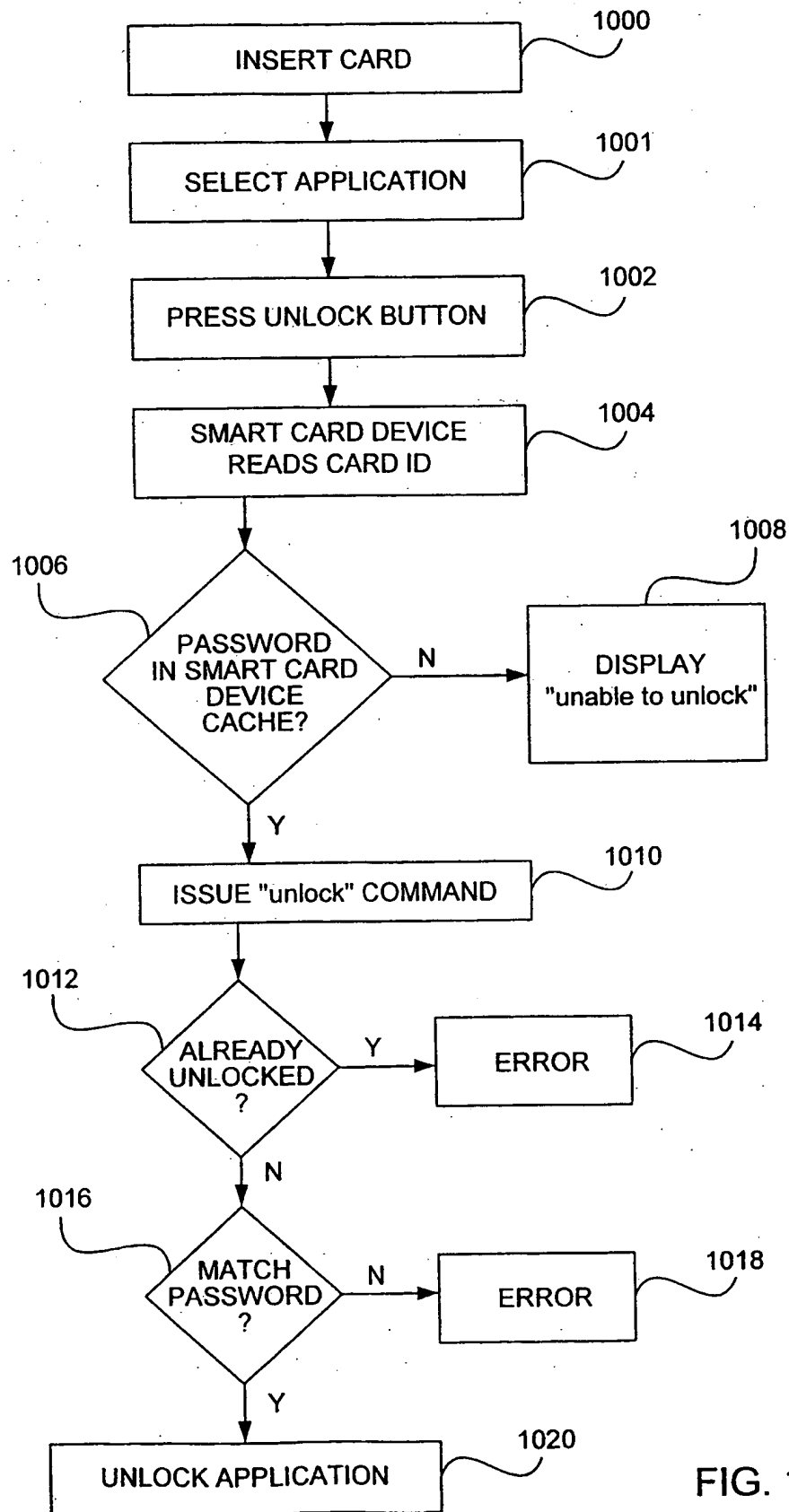


FIG. 12

COMMAND LOCK

	CONTENT	LENGTH
CLA	'80'	1
INS	TBD	1
P1	'00'	1
P2	'00'	1
LC	'03'	1
	PASSWORD	3

FIG. 13A

RETURN CODES

SW1	SW2	MEANING
	'9000'	SUCCESSFUL OPERATION
	'9111'	APPLICATION WAS ALREADY UNLOCKED
	'9112'	UNABLE TO UNLOCK

FIG. 13B

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 99/04986

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 637 710 A (B+DEVELOPMENT) 13 April 1990 (1990-04-13) abstract; claims; figures	1-4,8, 11-13
A	WO 91 10971 A (UTVECKLING AB JONIC) 25 July 1991 (1991-07-25) abstract; claims; figures	1,2,8, 11,12
A	FR 2 665 279 A (Y.A.F. ASCHENBROICH) 31 January 1992 (1992-01-31) abstract; claims; figures page 7, line 17 - page 14, line 31	1,2,4, 6-8, 11-13
A	DE 36 32 294 A (SIEMENS) 7 April 1988 (1988-04-07) -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

19 August 1999

Date of mailing of the international search report

26/08/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

David, J

INTERNATIONAL SEARCH REPORT

Int. Application No.

PCT/US 99/04986

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 94 17498 A (ENCO-TONE) 4 August 1994 (1994-08-04) ---	
A	US 5 065 155 A (Y. OOGITA) 12 November 1991 (1991-11-12) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/04986

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
FR 2637710	A	13-04-1990	NONE	
WO 9110971	A	25-07-1991	CA 2073449 A,C AU 639443 B AU 5104990 A DE 69032858 D DE 69032858 T EP 0511204 A ES 2129021 T JP 5503380 T NO 305149 B US 5350907 A	16-07-1991 29-07-1993 05-08-1991 04-02-1999 05-08-1999 04-11-1992 01-06-1999 03-06-1993 06-04-1999 27-09-1994
FR 2665279	A	31-01-1992	NONE	
DE 3632294	A	07-04-1988	NONE	
WO 9417498	A	04-08-1994	IL 104422 A CA 2154158 A EP 0680646 A JP 8509560 T	31-03-1996 04-08-1994 08-11-1995 08-10-1996
US 5065155	A	12-11-1991	JP 1903902 C JP 2120921 A JP 6030040 B JP 2128210 A	08-02-1995 08-05-1990 20-04-1994 16-05-1990